## AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A computer system for controlling the unauthorized use of software, comprising:

a host processor;

a removable media reading device coupled to said host processor;

a non-volatile memory coupled to said host processor, said non-volatile memory including a predetermined location for storing a signature, wherein the non-volatile memory is located in basic input/output system (BIOS) circuitry of said computer system; and

a bootup program stored in said non-volatile memory, said bootup program configured such that upon execution by said host processor the computer system will only be configured to decode encoded media in said removable media reading device if said signature is located in said predetermined location.

2. (Currently Amended) A method of reading encoded data from a removable media device in a computer system, the method comprising:

initiating a request for data from the removable media reader;

determining whether the system is authorized to decode encoded data, the determining comprising reading a signature in a non-volatile memory in a basic input/output circuit;

if the system is authorized to decode encoded data, determining whether the first sector on the removable media is encoded; and

if the system is authorized to decode encoded data and the first sector on the removable media is encoded, decoding the requested data on the removable media.

3. (Original) The method of Claim 2, wherein determining whether the system is authorized to decode encoded data includes verifying that a signature is stored in the system in a predetermined memory location.

4. (Currently Amended) ~~The method of Claim 2~~,

A method of reading encoded data from a removable media device in a computer system, the method comprising:

initiating a request for data from the removable media reader;

determining whether the system is authorized to decode encoded data;

if the system is authorized to decode encoded data, determining whether the first sector on the removable media is encoded;

if the system is authorized to decode encoded data and the first sector on the removable media is encoded, decoding the requested data on the removable media; and

~~further comprising~~ if the decode ability is not set, passing data, whether encoded or not, to the system.

5. (Currently Amended) ~~The method of Claim 2~~

A method of reading encoded data from a removable media device in a computer system, the method comprising:

initiating a request for data from the removable media reader;

determining whether the system is authorized to decode encoded data;

if the system is authorized to decode encoded data, determining whether the first sector on the removable media is encoded;

if the system is authorized to decode encoded data and the first sector on the removable media is encoded, decoding the requested data on the removable media; and

~~further comprising~~ if the decode ability is set and the decoding is set OFF, passing data to the system from the removable media as it is requested.

6. (Currently Amended) A method of preventing unauthorized access to encoded content stored on removable media by a computer system running an operating system and having a removable media reader, the method comprising:

running a memory-resident program with a lockable decoding function to control the interaction between the operating system and the removable media reader;

scanning the computer system for a predetermined signature and unlocking said lockable decoding function if said signature is found, wherein said predetermined signature is stored in a basic input output system (BIOS) circuitry of said computer system;

examining a removable medium to determine whether it is encoded and enabling said lockable decoding function if the removable medium is encoded; and

decoding data from the removable medium if said lockable decoding function is enabled.

7. (Original) The method of Claim 6, wherein said memory-resident program is inserted between the operating system and a device driver for the removable media reader.

8. (Currently Amended) A method of preventing unauthorized access to encoded content stored on removable media by a computer system running an operating system and having a removable media reader, the method comprising:

running a memory-resident program with a lockable decoding function to control the interaction between the operating system and the removable media reader;

scanning the computer system for a predetermined signature and unlocking said lockable decoding function if said signature is found;

examining a removable medium to determine whether it is encoded and enabling said lockable decoding function if the removable medium is encoded; and

decoding data from the removable medium if said lockable decoding function is enabled;

~~The method of Claim 6~~, wherein said memory-resident program adds at least one modular driver between the operating system and the removable media reader.

9. (Cancelled)

10. (Original) The method of Claim 6, wherein said predetermined signature is stored in a non-volatile memory of a central processing unit of said computer system.

11. (Currently Amended) A method of preventing unauthorized access to encoded content stored on removable media by a computer system running an operating system and having a removable media reader, the method comprising:

inserting a driver with a lockable decoding function between the operating system and the device driver for the removable media reader to control the transfer of information between the operating system and the removable media reader;

scanning the computer system for a predetermined signature, and unlocking said lockable decoding function if said signature is found, wherein said predetermined signature is stored in a basic input / output system (BIOS) circuitry of said computer system;

examining a removable medium to determine whether it is encoded and enabling said lockable decoding function if the removable medium is encoded; and

decoding data from the removable medium if said lockable decoding function is enabled.

12. (Cancelled)

13. (Original) The method of Claim 11, wherein said predetermined signature is stored in a non-volatile memory of a central processing unit of said computer system.

14. (Currently Amended) A method of preventing unauthorized access to encoded content stored on removable media by a computer system running an operating system and having a removable media reader, the method comprising:

inserting a driver with a lockable decoding function between the operating system and the device driver for the removable media reader to control the transfer of information between the operating system and the removable media reader;

scanning the computer system for a predetermined signature, and unlocking said lockable decoding function if said signature is found;

examining a removable medium to determine whether it is encoded and enabling said lockable decoding function if the removable medium is encoded; and

decoding data from the removable medium if said lockable decoding function is enabled

~~The method of Claim 11~~, wherein said examination of a removable medium to determine whether it is encoded further comprises: trapping insert status requests of the removable media reader from the operating system to the device driver of said removable media reader.

15. (Currently Amended) A method of preventing unauthorized access to encoded content stored on removable media by a computer system running an operating system and having a removable media reader, the method comprising:

inserting a driver with a lockable decoding function between the operating system and the device driver for the removable media reader to control the transfer of information between the operating system and the removable media reader;

scanning the computer system for a predetermined signature, and unlocking said lockable decoding function if said signature is found;

examining a removable medium to determine whether it is encoded and enabling said lockable decoding function if the removable medium is encoded; and

decoding data from the removable medium if said lockable decoding function is enabled

~~The method of Claim 11~~, wherein said decoding of data from the removable medium further comprises: trapping read requests from the operating system to the device driver of said removable media reader.

16. (Currently Amended) A method of preventing unauthorized access to encoded content stored on removable media by a computer system running an operating system and having a removable media reader, the method comprising:

adding at least one modular driver between the operating system and the removable media reader to incorporate a lockable decoding function to control the transfer of information between the operating system and the removable media reader;

scanning the computer system for a predetermined signature and unlocking said lockable decoding function if said signature is found, wherein said predetermined signature is stored in a basic input/output system (BIOS) circuitry of said computer system;

examining a removable medium to determine whether it is encoded and enabling said lockable decoding function if the removable medium is encoded; and

decoding data from the removable medium if said lockable decoding function is enabled.

17. (Cancelled)

18. (Original) The method of Claim 16, wherein said predetermined signature is stored in a non-volatile memory of a central processing unit of said computer system.

19. (Currently Amended) A method of preventing unauthorized access to encoded content stored on removable media by a computer system running an operating system and having a removable media reader, the method comprising:

adding at least one modular driver between the operating system and the removable media reader to incorporate a lockable decoding function to control the transfer of information between the operating system and the removable media reader;

scanning the computer system for a predetermined signature and unlocking said lockable decoding function if said signature is found;

examining a removable medium to determine whether it is encoded and enabling said lockable decoding function if the removable medium is encoded; and

decoding data from the removable medium if said lockable decoding function is enabled

~~The method of Claim 16~~, wherein the lockable decoding function is incorporated by adding an upper filter modular driver with said lockable decoding function.

20. (Currently Amended) A method of preventing unauthorized access to encoded content stored on removable media by a computer system running an operating system and having a removable media reader, the method comprising:

adding at least one modular driver between the operating system and the removable media reader to incorporate a lockable decoding function to control the transfer of information between the operating system and the removable media reader;

scanning the computer system for a predetermined signature and unlocking said lockable decoding function if said signature is found;

examining a removable medium to determine whether it is encoded and enabling said lockable decoding function if the removable medium is encoded; and

decoding data from the removable medium if said lockable decoding function is enabled

~~The method of Claim 16~~, wherein said examination of a removable medium to determine whether it is encoded further comprises:

trapping insert status requests of the removable media reader from the operating system to the class function driver of said removable media reader.

21. (Currently Amended) A method of preventing unauthorized access to encoded content stored on removable media by a computer system running an operating system and having a removable media reader, the method comprising:

adding at least one modular driver between the operating system and the removable media reader to incorporate a lockable decoding function to control the transfer of information between the operating system and the removable media reader;

scanning the computer system for a predetermined signature and unlocking said lockable decoding function if said signature is found;

examining a removable medium to determine whether it is encoded and enabling said lockable decoding function if the removable medium is encoded; and

decoding data from the removable medium if said lockable decoding function is enabled

~~The method of Claim 16~~, wherein said decoding of data from the removable medium further comprises:

trapping read requests from the operating system to the class function driver of said removable media reader

22. (Currently Amended) A method of preventing unauthorized access to encoded content stored on removable media by a computer system running an operating system and having a removable media reader, the method comprising:

programming the firmware of the removable media reader to incorporate a lockable decoding function to control the transfer of information between the operating system and the removable media reader;

scanning the computer system for a predetermined signature, and unlocking said lockable decoding function if said signature is found, wherein said predetermined signature is stored in a basic input/output system (BIOS) circuitry of said computer system;

examining a removable medium in the removable media reader to determine whether it is encoded, and enabling said lockable decoding function if the removable medium is encoded; and

decoding data from the removable medium if said lockable decoding function is enabled.

23. (Cancelled).

24. (Original) The method of Claim 22, wherein said predetermined signature is stored in a non-volatile memory of a central processing unit of said computer system.

25. (Original) The method of Claim 22, wherein said unlocking and said enabling of said lockable decoding function is performed by a memory-resident program.

26. (Currently Amended) A computer system for preventing unauthorized access to encoded content stored on removable media, comprising:

a removable media reader; and

a host processor running an operating system, said host processor coupled to said removable media reader and configured to

control the transfer of information between the operating system and the removable media reader with a lockable decoding function,

scan for a predetermined signature and unlock said lockable decoding function if said signature is found, wherein said predetermined signature is stored in a basic input/output system (BIOS) circuitry of said computer system,

examine a removable medium in said removable media reader to determine whether it is encoded and enable said lockable decoding function if the removable medium is encoded, and

decode data from the removable medium if said lockable decoding function is enabled.